Patent
Old Attorney Dkt. No. 027557-071
Attorney Docket No. 0119-082

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	**MAIL STOP Appeal Brief – Patents**
	)	
Stefan ANDERSSON	)	Group Art Unit: 2137
	)	
Application No.: 09/977,192	)	Examiner: WILLIAMS, Jeffery L.
	)	
Filed: October 16, 2001	)	Confirmation No.: 3198
	)	
For: SECURITY SYSTEM	)	

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal was filed on July 26, 2006. In support of that Appeal, this Appeal Brief is being filed concurrently with the required fee specified by 37 C.F.R. §41.20(b)(2). As the due date for this Appeal Brief is determined to be one month from the mailing date of the Notice of Panel Decision from Pre-Appeal Brief Review (i.e., one month from October 3, 2006), this Appeal Brief in conjunction with the Petition for One-Month Extension of Time plus applicable petition fees (filed concurrently herewith) is believed to be timely filed.

Favorable reconsideration and reversal of the various rejections are respectfully requested in view of the following remarks.

I. REAL PARTY IN INTEREST

The real party in interest in connection with this application is Telefonaktiebolaget L M Ericsson, by virtue of an Assignment executed by the inventor (Stefan ANDERSSON) on January 7, 2002, and recorded in the U.S. Patent and Trademark Office at Reel 012476, Frame 0738.

II. RELATED APPEALS AND INTERFERENCES

Applicant is unaware of any related appeals or interferences in connection with this application.

III. STATUS OF CLAIMS

Claims 20-23 and 31 have been canceled. The remaining claims 1-19, 24-30, and 32-50 stand rejected. The rejection of claims 1-19, 24-30, and 32-50 is appealed.

IV. STATUS OF AMENDMENTS

Applicant filed an After-Final Amendment on July 25, 2006 with proposals to amend a number of paragraphs of the specification. An Advisory Action mailed on August 4, 2006 informs that the proposed amendments will not be entered because they allegedly raise the issue of new matter.

V. SUMMARY OF CLAIMED SUBJECT MATTER

As explained in the application at page 1, line 11 through page 2, line 4, it is known to provide cryptographic functionality to support an application (e.g., e-mail or internet browser) which requires cryptography in a computer. As an example, U.S. Patent No. 5,689,565 describes a cryptography system architecture for a computer. The cryptography system has a cryptographic application program interface (CAPI) which interfaces with the application to receive requests for cryptographic functions. The system further includes at least one cryptographic service provider (CSP) that is independent from, but dynamically accessible by, the CAPI. The CSP provides the cryptographic functionality and manages the secret cryptographic keys.

This system architecture is used in many applications in which data may desirably be transferred across unsecured computer networks such as the internet. For example, this

architecture can be used in applications such as e-mail clients, web browsers, and the like. A similar architecture can be used for access control within a computer system, and for hard disc encryption.

It is advantageous not to maintain cryptographic keys and/or algorithms on the same computer hardware as the application(s) because anyone with unauthorized access to the computer would have access to these as well. Solutions known at the time of Applicant's invention suffer from a drawback in that, in addition to the computer, the user is required to carry with him/her extra equipment, such as an IC card and/or an IC card reader capable of connecting to the computer. The IC card is used for storing the cryptographic keys used by the CSP in the computer.

Applicant's invention addresses this problem, thereby reducing the burden on users, by establishing a synergistic relationship between the computer and another device that the user would ordinarily be carrying regardless of any planned computer usage: a mobile station (e.g., a cellular telephone). As explained in the specification at page 4, line 29 through page 5, line 21, mobile stations typically include their own cryptographic module for enabling encrypted communication over a wireless interface with a network, such as through a Wireless Application Protocol (WAP) Gateway. Encryption in these cases provides confidentiality for users.

Thus, as explained in the specification at page 5, line 22-28, in accordance with embodiments of the invention, the cryptographic module of the phone, and other features which are used to provide secure communication using the Wireless Application Protocol, also allow the mobile station (e.g., phone 30) (see FIGS. 1, 4, and 5) to provide some or all of the functionality of a cryptography service provider to the computer. In this way, the need to carry extraneous equipment just to perform the computer's cryptographic functions is eliminated. Instead, the computer determines that it requires cryptographic services, and establishes a connection to the mobile station to obtain these services (e.g., FIG. 2, steps 100-108). The requested cryptographic operation is carried out (e.g., FIG. 2, step 110; and FIG. 3, step 136), and the result of the cryptographic operation is passed from the phone back to the computer (e.g., FIG. 3, step 138). The computer then ensures that the application requesting the cryptographic operation receives the result of that operation (e.g., FIG. 2, steps 112-114), and the computer carries on its own operations without the need to further involve the mobile station.

Various embodiments defined by the claims will now be described with reference to the specification and drawings. It should be understood that any such reference (e.g., to specification text and/or elements/steps illustrated in the figures) is intended to be exemplary only. No inference should be made that the elements/steps being discussed are not also described and/or illustrated in other places of the application, possibly in connection with other embodiments.

Accordingly, embodiments defined by independent claim 1 are directed to:

1. A method of encrypting communications from a computer (e.g., the computers 10, 60) having an application program interface (e.g., CAPI 18), the method comprising:

initiating communications from said computer over a computer network (e.g., specification at page 3, lines 26-30);

determining that encryption of said communications is required (e.g., specification at page 3, line 31 through page 4, line 8);

establishing a connection with a mobile communications device (e.g., specification at page 6, lines number 1-4; FIG. 1: connection between CSP*26 and MS 30; FIG. 2: step 104; FIG. 4: connection between CSP*26 and MS 30; FIG. 5: connection between CT* 76 and MS 30; and FIG. 6: step 164), wherein said mobile communications device includes a cryptographic module for use in mobile communication over a wireless communications network (e.g., specification at page 5, lines 12 -21; FIG. 1: SIM-WIM 32; FIG. 4: SIM-WIM 32; FIG. 5: SIM-WIM 32); and

using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer (e.g., specification at page 7, line 33 through page 8, line 3; FIG. 2: steps 108-110; page 11, through page 12, line 4; and FIG. 6: steps 166-168) over said computer network without sending said encrypted communications over said wireless communications network (e.g., specification at page 8, lines 4-7 and FIG. 2: steps 112-114; specification at page 12, lines 5-8; and FIG. 6: step 170).

Embodiments defined by independent claim 7 are directed to:

7. A mobile communications device, comprising:

means for communicating over a wireless interface with a wireless communications network (e.g., specification at page 4, lines 20-33);

means for connection to a remote computer without involving the wireless communications network (e.g., specification at page 3, lines 26-30); and

a cryptographic module (e.g., SIM-WIM 32), the cryptographic module being usable:

for encoding wireless communications from the device over said wireless interface (e.g., specification at page 5, lines 6-21);

by a cryptographic service provider with an application program interface of the remote computer (e.g., specification at page 5, lines 22-28).

It is noted that the "means for communicating over a wireless interface" and the "means for connection to a remote computer" are defined in terms of means-plus-function as permitted by 35 U.S.C. §112, sixth paragraph. Exemplary supporting structure/material/acts for these elements are described in the application as indicated above.

Embodiments defined by independent claim 19 are directed to:

19. A tangible module for a personal computer (e.g., CSP* 26), wherein, in response to the module receiving a first command from a cryptographic application program interface, indicating that it requires cryptographic functionality for communication over a computer network (e.g., FIG. 2, steps 100-102), the module sends a second command to a mobile communication device (e.g., FIG. 2, step 104), the mobile communication device having a cryptographic module (e.g., SIM-WIM 32) for use in mobile communication over a wireless communications network, such that the cryptographic module acts as a cryptographic service provider for said personal computer (e.g., FIG. 2, step 110) allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network (e.g., FIG. 2 step 114 and specification at page 3, lines 26-30).

Embodiments defined by independent claim 24 are directed to:

24. A system, comprising:

a computer (e.g., PC 10); and

a mobile communications device (e.g., MS 30), including a cryptographic module (e.g., SIM-WIM 32) for performing cryptographic functions in mobile communication over a wireless communications network,

the computer having at least one application (e.g., e-mail application 14; browser 16) which requires cryptographic functionality for communication over a computer network,

a first part of the required cryptographic functionality being provided in the computer (e.g., SHA-1 algorithm functionality that can be provided on the CSP* 26 – see specification at page 6, lines 24-26), and a second part of the required cryptographic functionality being provided in the mobile communications device (e.g., RSA algorithm functionality that can be provided on the MS 30 – see specification at page 6, lines 26-28),

the computer and the mobile communications device having means for establishing a secure communications path therebetween (e.g., specification at page 6, lines 1-16); and

the computer further comprising an interface device (e.g., CAPI 18) which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto.

It is noted that the "means for establishing a secure communications path therebetween" (i.e., between the computer and the mobile communications device) are defined in terms of means-plus-function as permitted by 35 U.S.C. §112, sixth paragraph. Exemplary supporting structure/material/acts for these elements are described in the application as indicated above.

Embodiments defined by independent claim 28 are directed to:

28. A method of encrypting communications from a computer having an application program interface (e.g., CAPI 18), wherein the communications are over a computer network (e.g., specification at page 3, lines 26-30), the method comprising:

sending data to be encrypted from the computer to a mobile communications device (e.g., FIG. 2, step 108), wherein the mobile communications device has a cryptographic module (e.g., SIM-WIM 32) for performing cryptographic functions in communications over a wireless communications network (e.g., specification at page 5, lines 6-21), and further,

wherein the mobile communications device uses the cryptographic module to encrypt the data (e.g., specification at page 5, lines 22-28);

receiving encrypted data at the computer from the mobile communications device (e.g., FIG. 3, step 138); and

using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network (e.g., FIG. 2 step 114 and specification at page 3, lines 26-30).

Embodiments defined by independent claim 36 are directed to:

36. A system for supporting an application (e.g., e-mail application 14; browser 16), the system comprising:

a computer (e.g., PC 10) including:

a cryptographic application program interface (e.g., CAPI 18); and

a cryptography service provider (e.g., CSP* 26); and

a mobile communication device (e.g., MS 30) including a cryptographic module (e.g., SIM-WIM 32),

wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality for communication over a computer network, the cryptographic application program interface sends a command to the cryptography service provider (e.g., FIG. 2, steps 102-104), and

wherein the cryptography service provider has a communications link to the cryptographic module of the mobile communications device (e.g., specification at page 6, lines number 1-4; FIG. 1: connection between CSP*26 and MS 30; FIG. 2: step 104; FIG. 4: connection between CSP*26 and MS 30; FIG. 5: connection between CT* 76 and MS 30; and FIG. 6: step 164), the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface (e.g., specification at page 5, lines 12 - 21; FIG. 1: SIM-WIM 32; FIG. 4: SIM-WIM 32; FIG. 5: SIM-WIM 32), and

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications

over the telecommunications network (e.g., FIG. 2 step 114 and specification at page 3, lines 26-30).

Embodiments defined by independent claim 44 are directed to:

44. A mobile communications device (e.g., MS 30), the mobile communications device being able to communicate over a first wireless interface with a telecommunications network (e.g., specification at page 4, lines 20-33), and comprising a cryptographic module (e.g., SIM-WIM 32) to provide cryptographic functionality for use in communications over the first wireless interface, the mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface (e.g., Security Manager 38), wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module (e.g., FIG. 3, step 134), and returns the results of the cryptographic function to the computer system over the second interface, without sending the results of the cryptographic function over the first wireless interface (e.g., FIG. 3, step 138).

Embodiments defined by independent claim 47 are directed to:

47. A module for a computer system, the module comprising:

an application interface (e.g., CAPI 18) for connection to a computer application (e.g., e-mail application 14; browser 16); and

an external interface (e.g., FIG. 1: connection between CSP*26 and MS 30; FIG. 5: connection between CT* 76 and MS 30) for connection to a mobile communication device (e.g., MS 30) containing a cryptographic module (e.g., SIM-WIM 32);

wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom (e.g., specification at page 6, lines 17-28).

Claim 48 depends from 47 and further defines that "the module has some cryptographic functionality, and comprises means (e.g., CSP* 26; specification at page 6, lines 17-28) for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function." The "means for determining" are defined in terms of means-plus-function as permitted by 35 U.S.C. §112, sixth paragraph. Exemplary supporting structure/material/acts for these elements are described in the application as just indicated.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Applicant respectfully requests review of the following grounds of objection/rejection:

1. The objection to the specification as allegedly failing to provide proper antecedent basis for the claimed subject matter. (See 37 CFR 1.75(d)(1) and MPEP §608.01(o).) And, the rejection of claims 1-19, 28-30, and 32-46 under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement.

2. The rejection of claims 47 and 48 under 35 U.S.C. §102(b) as allegedly being anticipated by Caputo et al. (U.S. Patent 5,778,071) (hereinafter "Caputo").

3. The rejection of claims 1, 4, 6, 7, 11, 13-15, 18, 19, 24, 26-28, 32-34, 36-39, 42, and 44 under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of Liebenow et al. (U.S. Patent 6,131,136) (hereinafter "Liebenow").

4. The rejection of claims 5, 8, 9, 41, and 46 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of Ericsson, "Bluetooth -- A Global Specification for Wireless Connectivity" (hereinafter "Ericsson").

5. The rejection of claim 49 under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of Ericsson.

6. The rejection of claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of Geiger et al. (US Patent 6,463,534 B1) (hereinafter, "Geiger").

7. The rejection of claims 43 and 45 under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of RSA, "PKCS #11 v2.10: Cryptographic Token Interface Standard" (hereinafter "RSA").

8. The rejection of claim 50 under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of RSA.

VII. ARGUMENT

All of the objections and rejections set forth in the Final Office Action of May 3, 2006 are traversed in the following arguments:

1. **The specification provides proper antecedent basis for the claimed subject matter as required under 37 CFR 1.75(d)(1), and satisfies the written description requirement under 35 U.S.C. §112, first paragraph**

In the Final Office Action, the Examiner objected to the specification on the grounds that the specification does not provide antecedent basis for a number of limitations added to claims 1, 7, 19, 28, 36, and 44 in Applicant's Amendment filed on January 5, 2006. Additionally, claims 1-19, 28-30, and 32-46 were rejected under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement. The Examiner's entire explanation of this rejection was: "See objection to specification." Because the rejection under the first paragraph of Section 112 appeared to be based on the lack of antecedent basis cited above with respect to the objection to the specification, these two issues are discussed herein together.

In order to reduce the number of issues to be resolved on Appeal, Applicant filed an After-Final Amendment on July 25, 2006, in which it was proposed to amend the specification to provide antecedent basis for terminology used to describe elements/steps in the claims, which elements/steps were already supported by the originally-filed application. (See, e.g., Figs.1-3 and the supporting text spanning page 3, line 19 through page 8, line 28 of the originally-filed application.)

It was believed that these amendments would address all of the Office's concerns except for one, namely, the concern that "... the specification does not provide antecedent basis for the added limitation '*a computer including: ... a mobile communication device including a cryptographic module*', claimed within the amended claim 36." In response to this objection, Applicant's remarks noted that the Examiner had erred in parsing the claim. As amended, claim 36 does *not* define the computer as including a mobile communication device. Rather, claim 36 defines "A system ...comprising: a computer ....; and a mobile communication device." That is, the claimed system comprises two distinct elements (i.e., the computer and the mobile communication device) which are separate from one another. The specification is replete with support for this arrangement. (See, e.g., Fig. 1.) Consequently, no further amendments to the specification were believed to be necessary to address this aspect of the Office's concern.

Having addressed the Examiner's stated concerns (i.e., lack of antecedent basis in the specification) upon which were based the objection to the specification and the rejection of claims under 35 U.S.C. §112, first paragraph, Applicant was surprised to receive an Advisory Action explaining that the proposed amendments to the specification would not be entered on the grounds that "they raise the issue of new matter," because Applicant would have expected the issue of new matter to be raised with respect to the claims in the Final Office Action. Nonetheless, Applicant will now address the issues of antecedent basis as well as new matter.

Because Applicant's proposed amendments to the specification were not entered, the specification does not include word for word support of the language presently recited in claims 1, 7, 19, 28, 36, and 44. However, it is well known that "the invention claimed does not have to be described in *ipsis verbis* in order to satisfy the description requirement of Sec. 112." In re Wright, 866 F.2d 422, 424 (Fed. Cir. 1989). Instead, it is sufficient if "the meaning of [the claim language in question] is sufficiently described in the specification to inform the public what said language is intended to encompass." *Id.*

It is respectfully asserted that the meaning of the claim language introduced in the amendment of January 5, 2006 was sufficiently described in the specification to satisfy all statutory requirements. In particular, the last paragraph of claim 1 was amended as follows:

> using the cryptographic module of the mobile communications device[[,]] as a cryptographic service provider for encrypting said communications from

said computer over said computer network without sending said encrypted communications over said wireless communications network.

Claim 7 was similarly amended to define "means for connection to a remote computer without involving the wireless communications network."

Claim 19 was amended to define:
the mobile communication device having a cryptographic module for use in mobile communication over a wireless communications network, such that the ~~mobile communications device~~ cryptographic module acts as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network

Claim 28 was amended to define "using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network."

Claim 36 was amended to define:

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications over the telecommunications network.

And claim 44 was amended to define:

wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second

interface, without sending the results of the cryptographic function over the first wireless interface.

In each instance, the Examiner objected that the specification does not support claims that include a mobile communications device performing the cryptographic function for the computer without sending the results of the cryptographic function over the wireless network.

This objection is without merit. For example, the specification at page 3, lines 26-30, expressly states that "[t]he computer has a connection to an external network 12, for example through a modem (not shown)." The connection to the network 12 is illustrated in FIG. 1, and it can clearly be seen that the connection does not involve the mobile station 30.

The text spanning page 3, line 31 through page 4, line 19 clearly sets forth an intention to provide cryptographic functionality to applications running in the computer, which applications are communicating with the network 12 via the computer's own connection to that network.

A solution, described in the specification text spanning page 4, line 20 through page 8, line 28 involves a mobile station 30 providing the desired cryptographic functionality for the computer. As described on page 6, lines 1-16, there is a communication link established between the computer and the mobile station so that the computer can request the desired functionality, and the mobile station can return the desired results.

It is clear from the description that the mobile station does not pass the cryptographic results on to its own wireless network, but rather returns these results to the computer. For example, FIG. 2 is a flowchart showing a method by which the PC 10 can use the cryptographic functionality in the mobile phone 30. As explained on page 8, lines 4-7 of the specification, "In step 112, the result of the operation in the MS 30 is sent to the CSP*26, and then to the CAPI 18. In step 114, the CAPI 114 [sic: 18], then responds to the application which requested the cryptographic functionality."

Since the application that requested the cryptographic functionality is using the computer's own connection to the network 12 (see e.g., FIG. 1), there is no need for the encrypted data to pass back through the mobile phone 32 to the wireless network. Thus, no such action is described in the specification.

That the mobile communications device performs the cryptographic function for the computer without sending the results of the cryptographic function over the wireless network

is further supported by the specification text at page 8, lines 8-28, in conjunction with FIG. 3, which is a flowchart showing the operation carried out in the MS 30. Of relevance here is that the MS 30 carries out the requested cryptographic operation (step 136), and "[t]hen, in step 138, the result of the cryptographic operation is sent back to the PC over the previously established communication link." It will be observed that sending the cryptographic operation result back to the PC is the final step carried out in the MS 30, because there is no need for the MS 30 to involve its own wireless network.

It should be clear from the foregoing remarks that the various instances of claim language defining a mobile communications device performing a cryptographic function for a computer without sending the results of the cryptographic function over the wireless network are well-supported in the specification.

As to the Examiner's additional allegation that "... the specification does not provide antecedent basis for the added limitation '*a computer including: ... a mobile communication device including a cryptographic module*', claimed within the amended claim 36," Applicant again respectfully asserts that the Examiner has erred in parsing the claim. As amended, claim 36 does not define the computer as including a mobile communication device. Rather, claim 36 defines "A system ...comprising: a computer ....; and a mobile communication device." That is, the claimed system comprises two distinct elements (i.e., the computer and the mobile communication device) which are separate from one another. The specification is replete with support for this arrangement. (See, e.g., Fig. 1.) Consequently, no further amendments to the specification are believed to be necessary to address the Office's concern.

Accordingly, the objection to the specification as lacking antecedent basis, and the rejection of claims 1-19, 28-30, and 32-46 under the first paragraph of 35 U.S.C. §112 (regardless of whether the basis for the rejection is lack of antecedent basis or an allegation of new matter) should be reversed.

2. **Claims 47 and 48 are not anticipated under 35 U.S.C. §102(b) by Caputo et al. (U.S. Patent 5,778,071) (hereinafter "Caputo") because they each define subject matter that is neither found nor suggested in Caputo**

Claim 47 defines "A module for a computer system, the module comprising: an application interface ...; and an external interface for connection to a mobile communication device containing a cryptographic module; *wherein, when the module receives from the*

application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom." (Emphasis added.)

Claim 48 depends from 47 and further defines that "the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function."

Neither of claims 47 and 48 is anticipated by Caputo because Caputo fails to disclose or suggest a division of cryptographic functions wherein some are performed within the computer itself and others are performed within a cryptographic module located in a mobile communications device so that the computer comprises "a cryptographic module; wherein, *when the module receives from the application interface a request for a cryptographic function which the module is unable to provide*, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom," as defined by claim 47. Caputo is similarly silent with respect to claim 48's recitation of "the module [having] some cryptographic functionality, and compris[ing] means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function."

The Office Action of August 5, 2005 had alleged that the Caputo patent, at column 15 lines 13-39, discloses a computer comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto. In response to this allegation, Applicant pointed out (in the Amendment of January 5, 2006) that the cited portion of Caputo merely describes two modes of operation: one in which the device 10 encrypts the data and immediately sent it to the network 20, and another in which the device 10 performs the encryption but then returns the encrypted data to the computer 22 for subsequent transmission to the network 20, possibly as part of another message. Nowhere does this passage describe a computer having its own cryptographic capabilities separate and apart from those provided by the device 10.

The Final Office Action repeats the allegation that the subject matter of claims 47 and 48 is anticipated by the Caputo patent but appears to construe these claims as merely defining the computer sending commands to the cryptographic module. As to features such as "when

the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom," as defined by claim 47, and "the module [having] some cryptographic functionality, and compris[ing] means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function," as defined by claim 48, the Final Office Action states, on page 22, that "it is noted that the features upon which applicant relies ... are not recited in the rejected claim(s)." However, a reading of these claims shows that this is incorrect.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 47 and 48 under 35 U.S.C. §102(b) be reversed.

3. **Claims 1, 4, 6, 7, 11, 13-15, 18, 19, 24, 26-28, 32-34, 36-39, 42, and 44 define subject matter that is novel and nonobvious over Caputo in view of Liebenow et al. (U.S. Patent 6,131,136) (hereinafter "Liebenow")**

Embodiments defined by independent claims 1, 7, 19, 24, 28, 36 and 44 (as well as their related dependent claims 4, 6, 11, 13-15, 18, 26-27, 32-34, 37-39, and 42) are believed to be patentably distinguishable over the prior art of record because they include novel and nonobvious features that enable a single mobile communications device to achieve a unique efficiency in that *a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1.* In this respect, it is important to understand that the personal computer is *not* communicating *through* the mobile communications device and the wireless network to get to its own network; its exchanges with the mobile communications device are merely for the purpose of utilizing the cryptographic functions that the mobile communications device can offer.

Specific claimed features lacking in Caputo and Liebenow are discussed in the following sections A through E, followed by an additional discussion of why the Liebenow patent does not make up for the deficiencies of Caputo.

A. Neither Caputo nor Liebenow et al. (U.S. Patent 6,131,136) (hereinafter "Liebenow") disclose "establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication"

As mentioned earlier, an aspect of the variously claimed embodiments is that a single mobile communications device is able to achieve a unique efficiency because *a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network,* but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1. To that end, independent claim 1 defines "establishing a connection with a mobile communications device, wherein said mobile communications device includes a *cryptographic module for use in mobile communication*," (emphasis added) and each of independent claims 7, 19, 24, 28, 36, and 44 uses the same or similar language to define a comparable feature. Neither of the Caputo or Liebenow documents discloses or suggests this feature.

In support of its rejection, the Final Office Action asserts that Caputo discloses this claimed feature at figure 3; column 9, lines 46-60; column 15, lines 13-39; column 2, lines 23-27; and column 3, lines 33-38.

Applicant respectfully disagrees because the cryptographic circuitry disclosed by Caputo is not "for use in mobile communication over a wireless communications network" as variously required by the claims. Instead, the Caputo device requires a wired connection to a network. (See, e.g., Fig. 2 and column 5, lines 62-65: "Further, the connector port 14 is a modular receptacle which may be directly connected to a data transfer path, such as a telephone system.") Thus, there would be absolutely no need for Caputo's cryptographic circuitry to be for use in mobile communication over a wireless communications network.

Liebenow fails to make up for the deficiencies of Caputo at least because it does not even discuss cryptography. Consequently, any combination of Caputo with Liebenow would still lack this feature.

B. Neither Caputo nor Liebenow disclose "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network"

As mentioned earlier, an aspect of the variously claimed embodiments is that a single mobile communications device is able to achieve a unique efficiency because a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1. When the mobile communications device is operating on its own behalf, its encrypted communications can be sent over the wireless communications link. However, when the mobile communications device is operating for the benefit of the computer, it merely returns the encrypted result to the computer without involving the wireless communications network. Independent claims 1, 7, 19, 28, 36, and 44 thus variously define "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network."

The Final Office Action asserts that Caputo discloses this feature at figure 3; column 9, lines 46-60; column 15, lines 13-39; column 2, lines 23-27; and column 3, lines 33-38. Applicant respectfully disagrees because, one principle of operation taught by Caputo is that Caputo's computer is connected to the network *through* the device 10 (see, e.g., Caputo et al.'s figure 2). Consequently, even if the Caputo device 10 were modified to have wireless mobile communications capability (i.e., communicating with a wireless network), the external device 10 of Caputo would still be the computer's only path to the network. Thus, the computer would have to use the hypothetically-modified wireless mobile communications device to access its computer network through the wireless communications network. Such use would be contrary to the requirement that the cryptographic module be used to "encrypt[] said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network." Liebenow fails to

make up for the deficiencies of Caputo at least because it, too, is a pass-through device, and does not suggest returning any cryptographic results to the attached computer.

C. Neither Caputo nor Liebenow disclose a dual-mode cryptographic module that is both "for use in mobile communication over a wireless communications network" and also "us[ed] ... as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network"

Independent claim 1 defines "a cryptographic module for use in mobile communication over a wireless communications network" and also "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network." Independent claims 7, 19, 24, 28, 36, and 44 variously define comparable features. Neither Caputo nor Liebenow discloses or suggests this feature, and any combination of these two teachings would similarly lack the claimed limitations.

The device of Caputo appears to operate in only one mode, namely, for the benefit of the external device (computer); it sits in-between the computer and the network, passing data from one to the other, and performs cryptographic functions as required by the node that the *computer* is connected to. Consequently, there is no dual mechanism in which the cryptographic module of the mobile communication device is "for use in mobile communication over a wireless communications network" and also for "[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network." Liebenow fails to make up for the deficiencies of Caputo because it is silent with respect to cryptography, and therefore cannot suggest a dual-mode cryptographic module as claimed.

D. Neither Caputo nor Liebenow disclose a system in which "a first part of the required cryptographic functionality [is] provided in the computer, and a second part of the required cryptographic functionality [is] provided in the mobile communications device"

Independent claim 24 further defines "a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device."

As explained earlier with respect to the rejection of claims 47 and 48, Caputo fails to disclose or suggest this claimed feature because it is silent with respect to any division of cryptographic functions wherein some are performed within the computer itself and others are performed within a cryptographic module located in a mobile communications device.

Also as mentioned earlier, the Final Office Action states, on page 22, that "it is noted that the features upon which applicant relies ... are not recited in the rejected claim(s)." However, a reading of claim 24 shows that this is incorrect.

Liebenow fails to make up for the deficiencies of Caputo because it is silent with respect to cryptography. Consequently, any combination of Caputo with Liebenow would still lack the claimed feature.

E. Neither Caputo nor Liebenow disclose a system in which "the computer further compris[es] an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto"

Claim 24 additionally defines "the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto." This feature is related to the feature discussed above in Section D, wherein a first part of the required cryptographic functionality is provided in the computer, and a second part of the required cryptographic functionality is provided in the mobile communications device. The claimed "interface" provides the

capability of selecting which of the two cryptographic functionality service providers will be used when needed.

As Caputo is lacking any disclosure of some cryptographic functionality being performed in the computer, and some cryptographic functionality being performed in the mobile communications device, it follows that Caputo does not describe an interface for selecting one of the two. Liebenow, which is silent with respect to cryptographic functionality, fails to make up for the deficiencies of Caputo.

F. Any combination of Caputo's teachings with the teachings of Liebenow would still lack features variously defined by Applicant's claims

The Final Office Action acknowledges that Caputo does not disclose, at least, a mobile communication device that is also usable over a wireless communications network, but relies on Liebenow as making up for this deficiency. This reliance is unfounded, at least for the reasons discussed above in Sections A through E.

Moreover, Applicant believes that Liebenow cannot be considered to disclose a mobile communication device, as that term is used in Applicant's specification. Instead, Liebenow discloses a dual mode modem that automatically switches between a wireless and wire-based communication modes using mode selection circuitry that detects when a wire-based communications network, such as a standard land-line telephone network, is coupled to the modem. Such a device fails to satisfy Applicant's variously-worded definitions of "said mobile communications device includ[ing] a cryptographic module for use in mobile communication over a wireless communications network." (See, e.g., independent claims 1, 7, 19, 24, 28, 36, and 44.) Rather, Liebenow's dual mode modem is more of a dumb, slave device that could never be used on its own; it would therefore never require its own cryptographic module *for use in mobile communication over a wireless communications network*, as required by Applicant's claims. Consequently, any combination of Caputo with Liebenow would still lack this claimed feature.

Moreover, even if Caputo's device were modified to include Liebenow's dual mode capability, the combination would still operate in only one mode, namely, for the benefit of the external device (computer), operating only to pass data between the computer and its network. All cryptographic functions would be performed only as required by the node that the *computer* is connected to, *and would pass through the device to the computer network.*

By contrast, embodiments such as those defined by independent claim 28 require that *the encrypting device return the encrypted data to the computer* for communication over a computer network without sending the encrypted data over the wireless communication network. See also independent claim 44, which defines "a mobile communications device ... comprising a security manager module ... *[that] returns the results of the cryptographic function to the computer system* ...." (Emphasis added.) Consequently, any combination of Caputo with Liebenow et al. would still lack any dual mechanism in which the cryptographic module of the mobile communication device is "for use in mobile communication over a wireless communications network" and also for "[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network."

G. Conclusion

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 1, 4, 6, 7, 11, 13-15, 18, 19, 24, 26-28, 32-34, 36-39, 42, and 44 under 35 U.S.C. §103(a) be reversed.

4. Claims 5, 8, 9, 41, and 46 define subject matter that is novel and nonobvious over Caputo and Liebenow in view of Ericsson, "Bluetooth -- A Global Specification for Wireless Connectivity" (hereinafter "Ericsson")

Claims 5, 8-9, 41, and 46 variously depend from independent claims 1, 7, 36, and 44 and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above. Furthermore, the Ericsson document, which was relied on by the Office merely for its disclosing the use of Bluetooth technology, also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with Liebenow and Ericsson would still lack the various combinations of elements defined by claims 5, 8, 9, 41, and 46.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 5, 8, 9, 41, and 46 under 35 U.S.C. §103(a) be reversed.

5. **Claim 49 defines subject matter that is novel and nonobvious over Caputo in view of Ericsson**

Claim 49 depends from independent claim 47 and is therefore patentably distinguishable over any combination of Caputo for at least the reasons discussed above. Furthermore, the Ericsson document, which was relied on by the Office merely for its disclosing the use of Bluetooth technology, also fails to disclose any of the above-identified features that are lacking in Caputo. Consequently, any combination of Caputo with Ericsson would still lack the combinations of elements defined by claim 49.

For at least the foregoing reasons, it is respectfully requested that the rejection of claim 49 under 35 U.S.C. §103(a) be reversed.

6. **Claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40 define subject matter that is novel and nonobvious over Caputo and Liebenow in view of Geiger et al. (US Patent 6,463,534 B1) (hereinafter, "Geiger")**

Claims 2-3, 10, 12, 16, 17, 25, 29-30, 35, and 40 variously depend from independent claims 1, 7, 24, 28, and 36 and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above with respect to these base claims. Furthermore, the Geiger document, which was relied on by the Office merely for its disclosing the use of the Wireless Application Protocol (WAP) (utilizing WTLS and a WIM), also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with Liebenow and Geiger would still lack the various combinations of elements defined by claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40 under 35 U.S.C. §103(a) be reversed.

7. **Claims 43 and 45 define subject matter that is novel and nonobvious over Caputo and Liebenow in view of RSA, "PKCS #11 v2.10: Cryptographic Token Interface Standard" (hereinafter "RSA")**

Claims 43 and 45 depend from independent claims 36 and 44, respectively, and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above with respect to these base claims. Furthermore, the RSA

document, which was relied on by the Office merely for its disclosing the use of PKCS #11 with AT commands, also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with Liebenow and RSA would still lack the various combinations of elements defined by claims 43 and 45.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 43 and 45 under 35 U.S.C. §103(a) be reversed.

8. Claim 50 defines subject matter that is novel and nonobvious over Caputo in view of the RSA document

Claim 50 depends from independent claim 47, and is therefore patentably distinguishable over Caputo for at least the reasons discussed above with respect to claim 47. Furthermore, the RSA document, which was relied on by the Office merely for its disclosing the use of PKCS #11 with AT commands, also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with RSA would still lack the combination of elements defined by claim 50.

For at least the foregoing reasons, it is respectfully requested that the rejection of claim 50 under 35 U.S.C. §103(a) be reversed.

9. Conclusion

Applicant has traversed all of the objections and rejections stated in the Final Office Action, and accordingly believes that the application is now in condition for allowance. It is therefore respectfully requested that all of the objections and rejections raised in the Final Office Action be reversed, and that a Notice of Allowance be mailed to Applicant.

As required under 37 CFR §41.37(c)(1), a Claims Appendix Is Attached Hereto. There is no need for either an Evidence Appendix or a Related Proceedings Appendix.

Respectfully submitted,

Potomac Patent Group PLLC

Date: November 24, 2006

By: /Kenneth B. Leffler, Reg. No. 36,075/
Kenneth B. Leffler
Registration No. 36,075

P.O. Box 270
Fredericksburg, Virginia 22404
703-718-8884

VIII. CLAIMS APPENDIX

The following claims are now pending in the application:

Claim 1 (previously presented): A method of encrypting communications from a computer having an application program interface, the method comprising:

initiating communications from said computer over a computer network;

determining that encryption of said communications is required;

establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication over a wireless communications network; and

using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network.

Claim 2 (original): A method as claimed in claim 1, wherein the mobile communications device is a WAP-enabled device.

Claim 3 (original): A method as claimed in claim 1, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

Claim 4 (previously presented): A method as claimed in claim 1, wherein the step of establishing a connection with the mobile communications device comprises establishing a wired connection between the mobile communications device and the computer.

Claim 5 (previously presented): A method as claimed in claim 1, wherein the step of establishing a connection with the mobile communications device comprises establishing a wireless connection between the mobile communications device and the computer.

Claim 6 (original): A method as claimed in claim 1, comprising:

when the application program interface requires cryptographic functionality, calling a cryptographic service provider function in the mobile communications device.

Claim 7 (previously presented): A mobile communications device, comprising:

means for communicating over a wireless interface with a wireless communications network;

means for connection to a remote computer without involving the wireless communications network; and

a cryptographic module, the cryptographic module being usable:

for encoding wireless communications from the device over said wireless interface;

by a cryptographic service provider with an application program interface of the remote computer.

Claim 8 (previously presented): A mobile communications device as claimed in claim 7, wherein the means for connection to the remote computer comprises a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer.

Claim 9 (previously presented): A mobile communications device as claimed in claim 8, wherein the short-range wireless communications transceiver uses Bluetooth wireless technology.

Claim 10 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is usable to support wireless communications using Wireless Transport Layer Security.

Claim 11 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module uses public key cryptography.

Claim 12 (original): A mobile communications device as claimed in claim 7, comprising means for sending and transmitting data using WAP.

Claim 13 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is realized in hardware in the device.

Claim 14 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is realized in software in the device.

Claim 15 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is provided on an external smart card.

Claim 16 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module comprises a Wireless Identity Module card.

Claim 17 (original): A mobile communications device as claimed in claim 16, wherein the cryptographic module comprises a Wireless Identity Module card which allows communications using Wireless Transport Layer Security.

Claim 18 (original): A mobile communications device as claimed in claim 7, comprising an interface for receiving a command from a personal computer, the mobile communications device acting as a cryptographic service provider for said personal computer in response to said command.

Claim 19 (previously presented): A tangible module for a personal computer, wherein, in response to the module receiving a first command from a cryptographic application program interface, indicating that it requires cryptographic functionality for communication over a computer network, the module sends a second command to a mobile communication device, the mobile communication device having a cryptographic module for use in mobile communication over a wireless communications network, such that the cryptographic module acts as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network.

Claims 20-23 (canceled)

Claim 24 (previously presented): A system, comprising:

a computer; and

a mobile communications device, including a cryptographic module for performing cryptographic functions in mobile communication over a wireless communications network,

the computer having at least one application which requires cryptographic functionality for communication over a computer network,

a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device,

the computer and the mobile communications device having means for establishing a secure communications path therebetween; and

the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto.

Claim 25 (original): A computer system as claimed in claim 24, wherein the mobile communications device is a WAP-enabled device.

Claim 26 (original): A computer system as claimed in claim 24, wherein the computer application which requires cryptographic functionality is an internal memory access application.

Claim 27 (original): A computer system as claimed in claim 24, wherein the computer application which requires cryptographic functionality is an external communication application.

Claim 28 (previously presented): A method of encrypting communications from a computer having an application program interface, wherein the communications are over a computer network, the method comprising:

sending data to be encrypted from the computer to a mobile communications device, wherein the mobile communications device has a cryptographic module for performing cryptographic functions in communications over a wireless communications network, and further, wherein the mobile communications device uses the cryptographic module to encrypt the data;

receiving encrypted data at the computer from the mobile communications device; and

using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network.

Claim 29 (original): A method as claimed in claim 28, wherein the mobile communications device is a WAP-enabled device.

Claim 30 (original): A method as claimed in claim 28, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

Claim 31 (canceled)

Claim 32 (original): A method as claimed in claim 28, comprising using a cryptographic module realized in hardware in the mobile communications device.

Claim 33 (original): A method as claimed in claim 28, comprising using a cryptographic module realized in software in the mobile communications device.

Claim 34 (original): A method as claimed in claim 28, comprising using a cryptographic module provided on an external smart card which can be read by the mobile communications device.

Claim 35 (original): A method as claimed in claim 28, comprising using a cryptographic module provided on a Wireless Identity Module card in said mobile communications device.

Claim 36 (previously presented): A system for supporting an application, the system comprising:

a computer including:

a cryptographic application program interface; and

a cryptography service provider; and

a mobile communication device including a cryptographic module,

wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality for communication over a computer network, the cryptographic application program interface sends a command to the cryptography service provider, and

wherein the cryptography service provider has a communications link to the cryptographic module of the mobile communications device, the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface, and

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications over the telecommunications network.

Claim 37 (original): A system as claimed in claim 36, wherein the cryptographic module is realized in hardware in the mobile communications device.

Claim 38 (original): A system as claimed in claim 36, wherein the cryptographic module is realized in software in the mobile communications device.

Claim 39 (original): A system as claimed in claim 36, wherein the cryptographic module is provided on an external smart card which can be read by the mobile communications device.

Claim 40 (original): A system as claimed in claim 36, wherein the cryptographic module is provided on a Wireless Identity Module card in said mobile communications device.

Claim 41 (original): A system as claimed in claim 36, wherein the cryptography service provider has a Bluetooth wireless communications link to the mobile communications device.

Claim 42 (original): A system as claimed in claim 36, wherein the cryptography service provider has some cryptographic functionality, and, on receipt of a command from the cryptographic application program interface, determines whether it can perform the required cryptographic functionality, or whether to obtain the required cryptographic functionality from the cryptographic module of the mobile communications device.

Claim 43 (original): A system as claimed in claim 36, wherein the communications link between the cryptography service provider and the cryptographic module of the mobile communications device uses a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

Claim 44 (previously presented): A mobile communications device, the mobile communications device being able to communicate over a first wireless interface with a telecommunications network, and comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface, the mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface, wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second interface, without sending the results of the cryptographic function over the first wireless interface.

Claim 45 (original): A mobile communications device as claimed in claim 44, wherein the security manager module responds to a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

Claim 46 (original): A mobile communications device as claimed in claim 44, wherein the second interface is a Bluetooth short-range radio interface.

Claim 47 (original): A module for a computer system, the module comprising:

an application interface for connection to a computer application; and

an external interface for connection to a mobile communication device containing a cryptographic module;

wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom.

Claim 48 (previously presented): A module for a computer system as claimed in claim 47, wherein the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function.

Claim 49 (original): A module for a computer system as claimed in claim 47, wherein the external interface is a Bluetooth short-range radio interface.

Claim 50 (original): A module for a computer system as claimed in claim 47, wherein the module sends over the external interface a command from a command set as defined in a standard PKCS#11, where the commands are redefined as AT commands.